6.0 SYSTEMS, DATABASE, AND SECURITY ADMINISTRATION

Administration is a critical part of GCCS. System administration, for purposes of this handbook, refers to the network communications administration and the information system administration functions, which are intertwined and mutually dependent, as are the physical network components and the hardware and software engines in the information system. GCCS, as a global, distributed processing system using client/server technology, relies heavily upon proper network management. The network, in turn, is highly reliant upon the software-based communications elements which it interfaces. Again, the network becomes the computer.

Administration is a complex, precise discipline and must be performed by highly qualified personnel. The following sections will highlight the major issues in administration:

- At the system level,
- For databases as a subset of the system, and
- For security, which is of paramount importance in the era of information warfare.

6.1 System Administration

This section discusses system-level administration and begins with a discussion of the WWMCCS to GCCS transition. Although administration is within the purview of specifically designated individuals, all GCCS users should generally understand the duties of the System Administrators, Database Administrators, and Network Managers, if only to know who to contact for help. For some small GCCS sites such as Secondary sites,[1] some of these duties will have to be performed by local C^4I operators or supported by personnel from other sites. GCCS administration will probably fit into the existing C^4I structure of the CINC or Service/Agency command operations already in place, and will be tailored to match command unique procedures.

6.1.1 WWMCCS/GCCS Transition. WWMCCS has been the foundation C^2 system for joint warfighting for more than 20 years. GCCS is replacing the WWMCCS functionality and adding significant new capabilities. WWMCCS and GCCS are radically different, although many WWMCCS applications migrated to GCCS as legacy subsystems may appear basically the same. For example, data rates on circuits connecting the GCCS sites are 10 times faster than WWMCCS interconnections, and GCCS servers are 100 times more powerful and faster than WWMCCS mainframes. Transaction flow for JOPES applications in GCCS use an improved broadcast distribution, versus the slow, congested daisy-chaining used in WWMCCS.

6.1.2 Transition Plans. The overall plan for transition is as follows. GCCS and WWMCCS will operate in parallel after GCCS Version 2.1 comes on-line at IOC. WWMCCS will use real-world data and stand ready to handle day-to-day and crisis situations. GCCS will be loaded with data to allow a formal period of User Assessment of GCCS to evaluate its functionality. Part of the assessment will include how well the new GCCS system and network management entities perform their roles in controlling the system. Three WWMCCS sites will be operated at the Top Secret (TS) level to provide a residual, temporary TS capability

---

[1] Secondary GCCS sites are those sites indirectly supporting a Unified of Specified command without the personnel or the technical expertise to manage the entire local GCCS operation. A site can be categorized as a Secondary GCCS site if they were supported by a remote WWMCCS Host. Secondary Sites are not expected to be manned and operational 24-hours a day, 7 days a week.

for GCCS. These sites are referred to as the Top Secret Support System (TS3). The TS Honeywell mainframes at these three sites are being replaced with Sun servers and a new system architecture. When completed, this capability will be referred to as GCCS(T). GCCS system and network management will be required at a Secret and Top Secret level.[2] When GCCS is assessed as ready, loaded with the current situational data, and achieves Final Operating Capability (FOC), it will be declared operational by the Joint Staff. WWMCCS can then be terminated, except for the TS3 sites.

6.1.3 Network and C² System Transition. Network communications supporting WWMCCS will also be changed in the GCCS environment, although changes are not just due to GCCS, but rather are part of the over-arching strategy for the DII. Changes in networks and the C² systems are summarized in Figure 6-1.

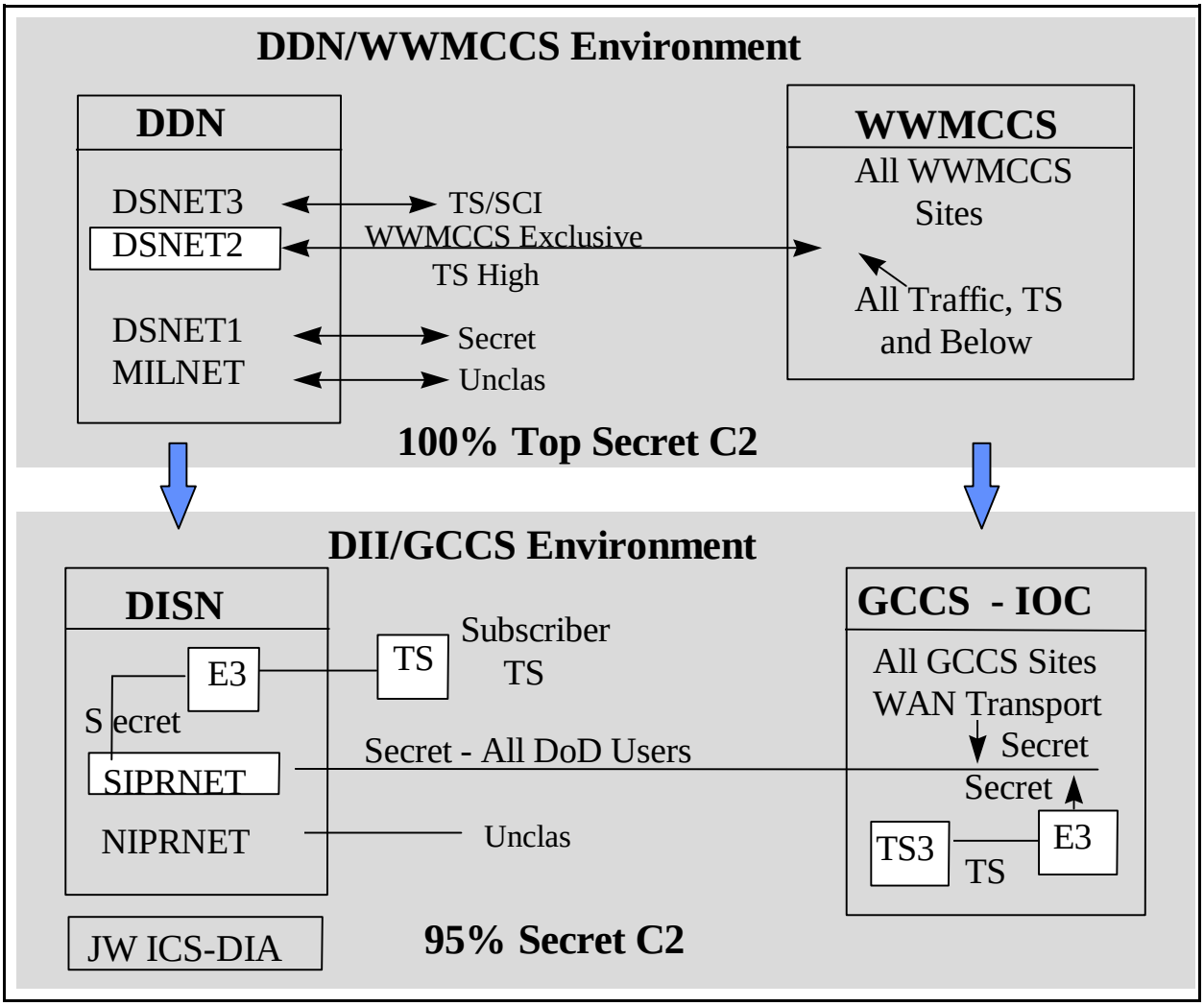

Figure 6-1. Network and C² System Transition

The four subsystems of the DDN packet switched network with the four levels of System High traffic will be

[2] Eventually, by using approved multilevel security technology and compartmented mode workstations, both levels will operate on a single platform.

replaced by the DISN NIPRNET at the Unclassified/Sensitive level and the SIPRNET at the Secret level. Subscribers with Top Secret requirements will use End-to-End Encryption (E3) devices to encrypt datagrams and then send the result over the Secret level SIPRNET. For GCCS, 95 percent of the traffic will be at the Secret level and will access the SIPRNET directly. The GCCS TS3 Top Secret level traffic will use the Motorola Network Encryption System (NES) E3 to encrypt and then send datagrams over the SIPRNET. The JWICS system, separate from the DISN and operated by DIA, will serve DoD users with residual TS/SCI requirements.

6.1.4 JOPES GCCS/WWMCCS Fallback Procedures. Procedures have been developed to allow users to switch back from GCCS to WWMCCS-only operations if needed during the period of GCCS operational assessment. Figure 6-2 shows the parallel operation for JOPES GCCS/WWMCCS after WWMCCS has been downgraded to Secret and the site GCCS LAN is connected to the WWMCCS LAN by Ethernet connection (for GCCS Core Database sites which are also WWMCCS JOPES Database sites).

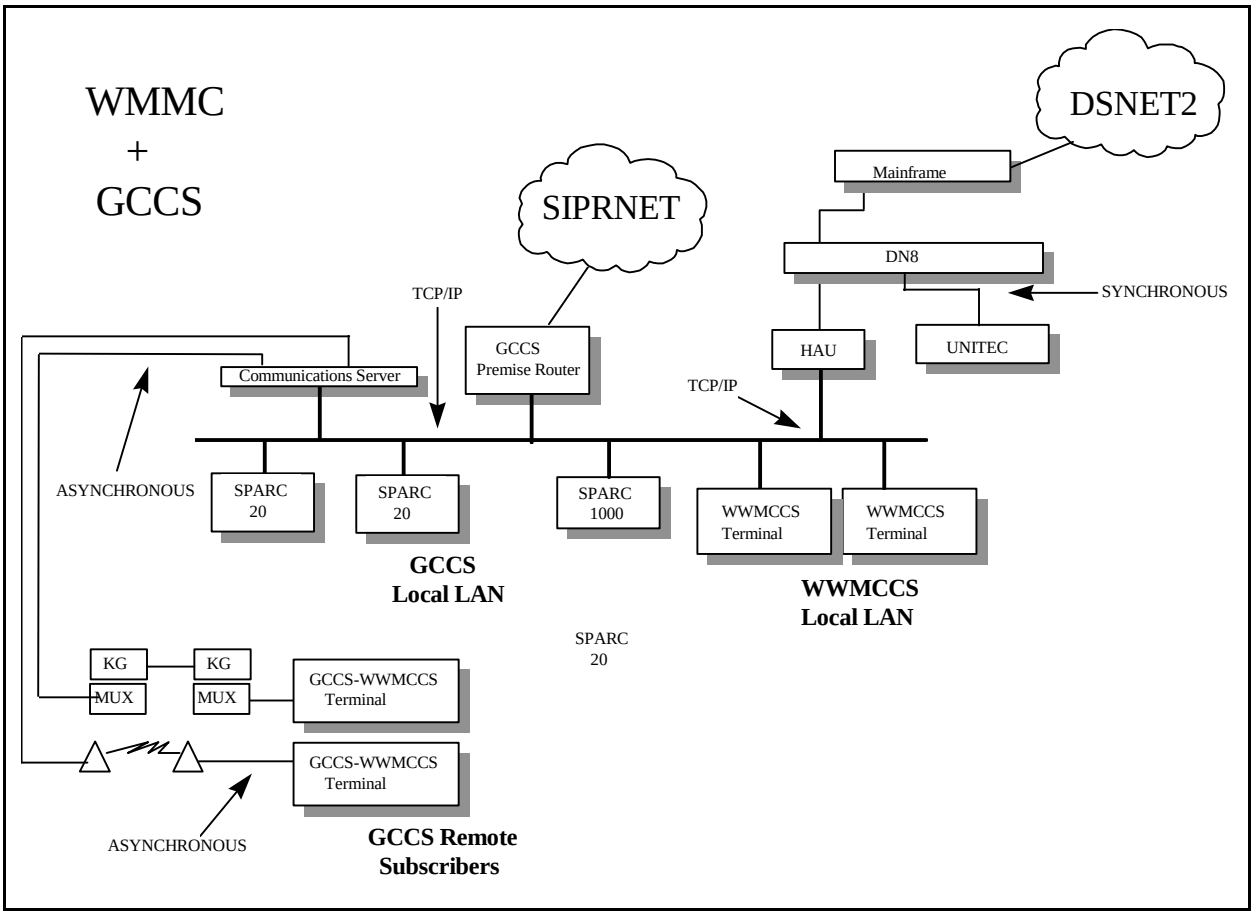

Figure 6-2. JOPES GCCS/WWMCCS Fallback Configuration

All GCCS clients establish access to the WWMCCS hosts via the VIP utility and/or GLINK during site installation. All GCCS JOPES users (local, remote, GUI, and CUI) check that access to WWMCCS host works via GLINK or the VIP 7705 emulator utility. The VIP utility is available from Desktop or RunRemote for the client. When the Joint Staff declares Fallback via AUTODIN message, the Joint Staff Support Center (JSSC), specifically the Technical Database Manager, publishes Fallback notice on the WWMCCS

JOPESTECH Teleconferencing Program and coordinates WWMCCS JOPES start-up. All JOPES users then access WWMCCS via the VIP utility or GLINK. When WWMCCS is finally turned off, all JOPES operations will be on GCCS using "GCCS-only" terminals.

6.1.5 System and Network Management Transition. WWMCCS relies on the WIN and its communications subsystem, called WINCS, for worldwide information transport. Many organizations are involved in managing the WWMCCS information system and the WIN. There are parallels in the management of WWMCCS and GCCS just as there are parallels in the system/network structure discussed in the previous sections. Figure 6-3 shows the parallelism and transition in roles and responsibilities necessary to manage the new GCCS/SIPRNET system/network.

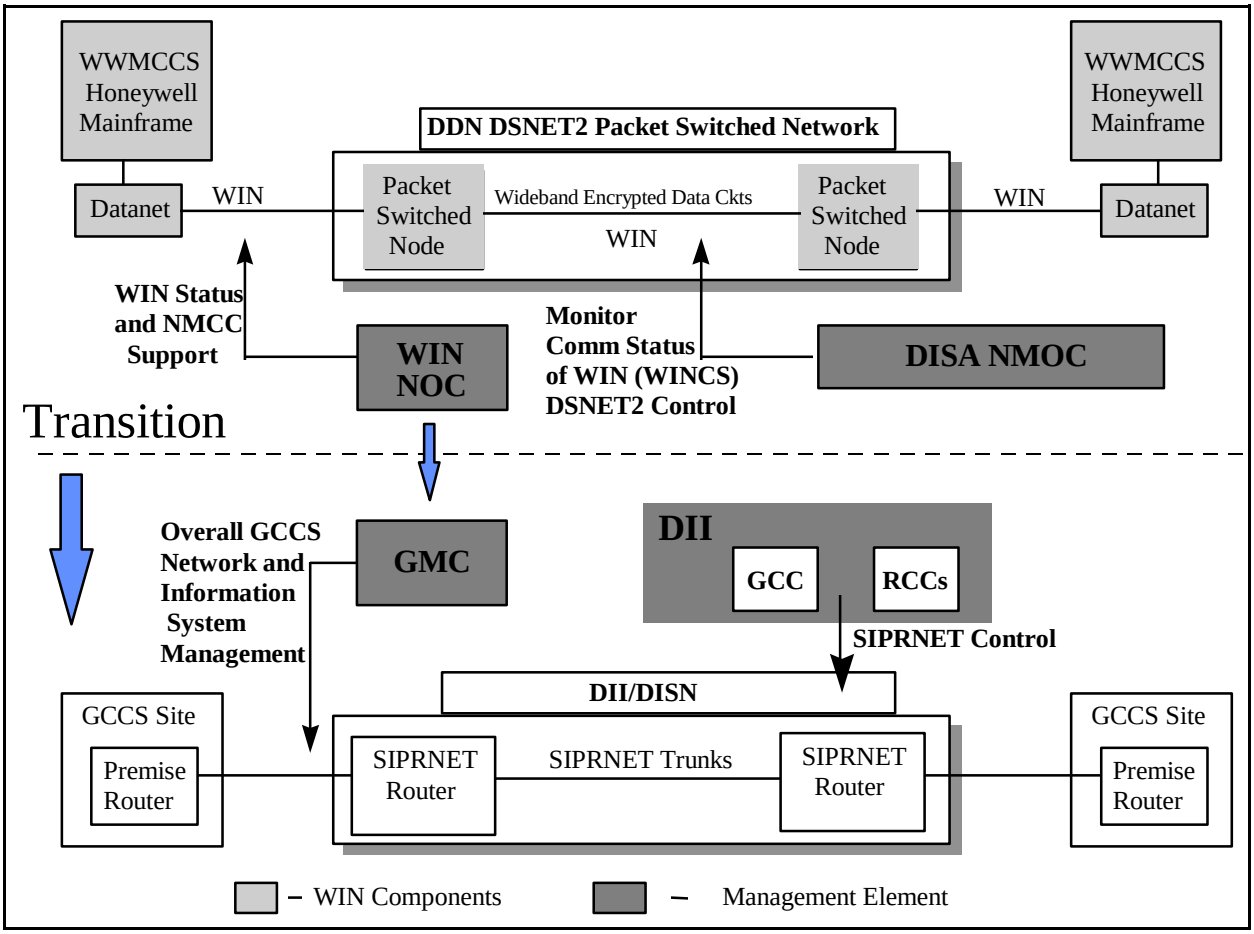

Figure 6-3. Transition of System and Network Management

Figure 6-3 only addresses the primary entities involved in managing and administrating WWMCCS and GCCS. Many other organizations are involved, especially at individual sites, that will be identified later. The organizations in Figure 6-3 are the chief elements in managing operations on the primary communications networks and the overall system level operations for WWMCCS and GCCS.

6.1.5.1 WWMCCS Intercomputer Network (WIN) Management. WIN architecture is the collection of Honeywell mainframes host computers, their WIN-dedicated Honeywell Datanets interconnected through Packet Switched Nodes (switching computers), and wideband, encrypted, dedicated computers. These

elements (and the remote terminals), combined with the controlling WIN Network Operations Center (WIN NOC) and the DISA Network Management Operations Center (NMOC), form the WIN. The communications portion is the WINCS. The NOC monitors the WIN to include overall network, host and Teleconference status and handles trouble reports. It also supports the NMCC. The DISA NMOC monitors and controls the communications assets within the DSNET2.

6.1.5.2 GCCS Management. GCCS is a virtual network of integrated information system servers operating across the DISN (SIPRNET) and managed by the GCCS Management Center (GMC). The GMC will perform all system management and network management (excluding DII functions) using COTS and Government off-the-shelf (GOTS) products. This includes management of all Joint applications running in GCCS. CINCs and Services/Agencies will manage their own unique applications. The SIPRNET will be controlled by the DISA Global Control Center (GCC) and the Regional Control Centers (RCCs) of the DII/DISN. As a common DoD user system, the net will be controlled to meet all DoD user requirements, not just GCCS site requirements. The GMC and the GCC must closely coordinate their activities. The GCC and RCCs (one in the Pacific, one in CONUS, and one in Europe) are DII assets to control the backbone SIPRNET. Subscribers are responsible for establishing primary and secondary Local Control Centers (LCCs). The GMC is established at three locations (see Figure 6-4), each of which will perform as a primary LCC for GCCS. CINC and Service/Agency GCCS sites will function as secondary LCCs, managing their own unique system/network infrastructures. This handbook addresses only the functions of the GMC. GCCS personnel at secondary LCCs must be knowledgeable of the required LCC functions.

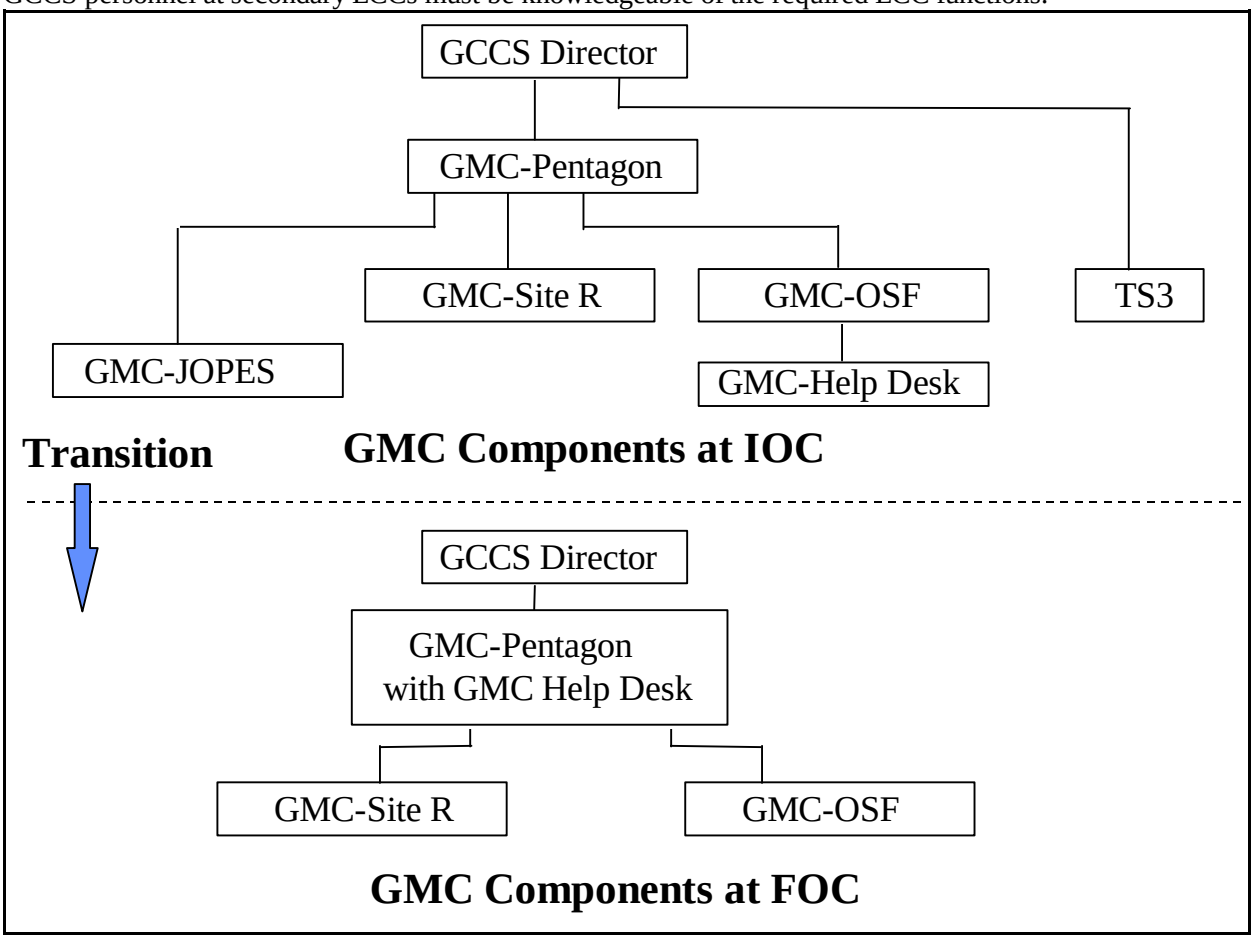

Figure 6-4. GMC Components at IOC and FOC

6.1.5.3 The GMC. The GMC will support all GCCS sites, the NMCC, and the functions of the JCS/J6 GCCS Director. It will operate 24-hours a day, 7 days a week. As shown in Figure 6-4, the GMC will consist of multiple components at IOC. The three main components are: the GMC-Pentagon, GMC-Site R at the ANMCC, and the GMC-OSF at the Operational Support Facility (OSF) in Sterling, Virginia. The GMC-Pentagon will be the main control center. GMC-Pentagon will report to the GCCS Director and will serve as the primary interface to GCCS sites and users and will be the center of all system and network management activities. It will be operated by the former WIN NOC staff. During routine operations, the GMC-Pentagon will limit itself to assisting and advising the GCCS sites. During Priority Mode operations, all GCCS sites' management functions will be subordinated to the GMC-Pentagon. The GMC-Pentagon will do all performance management, fault management, and security monitoring. The GMC-Pentagon will coordinate closely with the GCCS sites, DII GCC and RCCS, and the LCCs of the Service/Agencies.

The other GMC sites will be subordinate to the GMC-Pentagon, with the exception of the Top Secret TS3, which will initially remain under WWMCCS management. GMC-Site-R will be a fully capable back-up to the GMC-Pentagon. GMC-Site-R will be initially operated by DISA/WESTHEM/WEY personnel, who also man the Site-R WIN NOC. The GMC-OSF will be responsible for administration, planning, engineering, logistics, and provisioning. It will also have an operational role at IOC since it will contain the GMC-HelpDesk. In addition to the three main locations and the GMC-HelpDesk, the GMC-JOPES entity (operated by DISA/WESTHEM/WEY3 offices supporting JOPES) will also be part of the GMC at IOC. It will be responsible initially for system management of the JOPES applications on GCCS.

Each of the three primary GMC sites will require workstations for the GMC system and network management. The GMC-Pentagon and GMC-Site will also require database server space on the NMCC and ANMCC SPARCserver 1000s for holding management data. The GMC-OSF will operate as a client to the database server at the NMCC with the ANMCC database server acting as a back-up. Each of the three sites will require a suite of control hardware operating at the Secret level and a suite operating at the Top Secret level to control GCCS at IOC. Each site will have three client workstations for Secret management functions and two workstations for Top Secret management. The GMC sites also maintain all permissions and access codes necessary to perform their functions at the GCCS sites.

6.1.5.4 GMC-HelpDesk. The GMC-HelpDesk is the GCCS user's primary POC for all problems associated with the Joint Mission that cannot be locally resolved. The GMC-HelpDesk will not support CINC or Service/Agency unique applications. Any user may report problems but the user should first report to the GCCS Site Coordinator, who will try to solve the problem using local resources before contacting the GMC-HelpDesk. The GMC-HelpDesk is available initially to Secret-level GCCS users. A residual WWMCCS staff will provide support for the TS3 Top Secret portion of GCCS. When TS3 transitions to GCCS(T), a single GMC-HelpDesk will support both classification levels. The GMC-HelpDesk operates 24-hours a day, 7 days a week.

6.1.5.5 GMC at FOC. The final GMC configuration will see the incorporation of the GMC-JOPES entity into the GMC-Pentagon. After GCCS(T) is achieved, management of the Top Secret portion of GCCS will also be integrated into the GMC-Pentagon. Also, after GCCS is operational, WWMCCS is terminated, and other conditions are established, the GMC-HelpDesk will be moved from the GMC-OSF to the GMC-Pentagon. This will result in the configuration shown in Figure 6-4.

The GMC sites can be reached by telephone and are equipped with STU-IIIs for secure voice capability.

Table 6-1. GMC Telephone Directory (cont.)

Secure and unclassified FAX capability is also installed. Telephones operate against a rotary hunt group to ensure adequate accessibility. Pertinent GMC telephone numbers are provided in Table 6-1.

Table 6-1. GMC Telephone Directory

Location	Voice (DSN)	Voice (Commercial)	UNCLAS FAX (DSN)	SECURE FAX (DSN)	Beeper (Commercial)
GMC-Pentagon	227-4563	(703) 697-4563	227-3352	TBD	(202) 773-6965
GMC-Site R	988-3136	(301) 868-3136	988-3257	988-3552	N/A
GMC-OSF	653-8681	(703)-735-8681	653-8685	TBD	N/A
GMC-HelpDesk	653-8681	(703) 735-8681	653-8685	TBD	N/A
GMC-JOPES					
- TDBM	223-4438 223-4440	(703) 693-4438 (703) 693-4440	223-2957	TBD	(202) 773-9344
- FDBM	225-0022	(703) 695-0022	224-9630	TBD	(703) 512-2304 (202) 773-9289
TS3 (WWMCCS Infrastructure)	225-3025	(703) 695-3025	227-3352	TBD	(202) 773-6965

6.1.5.6 Summary. Managing GCCS is a complex task. Users are advised to read the *GCCS System and Network Management CONOPS*, Version 1.6, for additional background. It provides a detailed explanation of the specific functions performed by the GMC, descriptions of the COTS and GOTS products used to manage the GCCS assets, and presents the organizational and manning structure of the GMC sites. The information in Figure 6-5 shows the relationship of WWMCCS management organizations to GCCS management organizations.

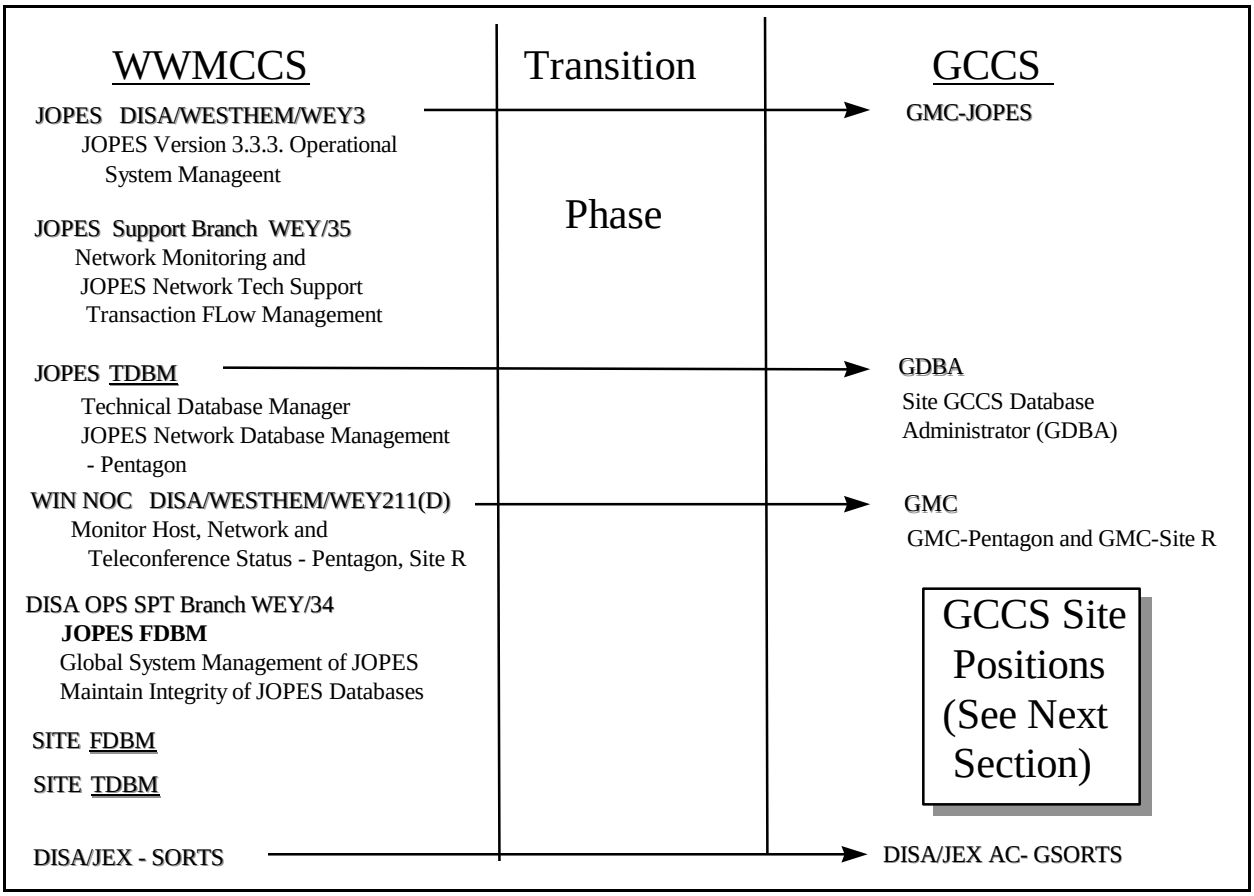

Figure 6-5. WWMCCS and GCCS System Management Organizations

Most of the roles of the various organizations are shown in Figure 6-5, with the exception of the WWMCCS TDBMs, FDBMs, and the SORTS managers. The duties of these entities are explained in more detail in the *GCCS System and Network Management CONOPS*. Section 6.2 addresses the GCCS environment, concentrating on the responsibilities of the GCCS site personnel charged with operating, maintaining, protecting, and managing the system.

6.2 GCCS Site Positions

The C^4I personnel structure of a typical GCCS site is shown in Figure 6-6. The functions of each position are discussed following the figure and focus on the GSA and the GDBA.

GSC	**GCCS Site Coordinator**
GNA	**GCCS Network Adminstrator**
GSA	**GCCS System Adminstrator**
GDBA	**GCCS Datbase Administrator**
DAA	**GCCS Site Designated Approving Authority**
SGSO	**Site GCCS Security Officer**
GSSP	**GCCS System Support Programmer**

Figure 6-6. GCCS Site Positions

6.2.1 GCCS Site Coordinator (GSC). The GSC is responsible for coordinating all system and network support activities within the GCCS site. The GSC is the primary focal point for coordinating with the GMC and other GCCS organizations. One major duty is to direct activities during and following an emergency to minimize loss of GCCS mission capabilities.

6.2.2 GCCS Network Administrator (GNA). The GNA is responsible for day-to-day operation of the GCCS LAN, the data and application servers, and the communications devices including the communications server, premise router and intelligent hubs, and related GCCS equipment. This includes maintaining and installing components on the LAN, operating the LAN, trouble shooting, maintaining TEMPEST and physical security requirements, and providing expertise in TCP/IP services.

6.2.3 GCCS System Administrator (GSA). The GSA has a major focus on maintaining the GCCS applications, providing local user support, and trouble shooting site problems with the GCCS applications. The key GCCS documents guiding the GSA are the *GCCS System Administration Manual*, the various application user manuals, and the documentation for commercial products such as the Oracle manuals. Some duties of the GSA are:

- Direct activities during and following an emergency to minimize loss of mission capability.
- Maintain access permission lists.
- Maintain the EM permissions program.
- Add and remove hardware and software at the local site.
- Perform system startups and back-ups.
- Administer software components of the LAN and WAN, including elements resident on the server.
- Generate periodic summaries of system performance and utilization.
- Routinely back up data and audit files.

- Set up the capability for administering GCCS user ID and password accounts. The Site Security Officer will use the account to establish and maintain IDs and passwords.
- Coordinate database modifications with other site personnel and the GMC-Pentagon.
- Diagnose system problems and report them to the GSC and GMC-HelpDesk.
- Monitor total system performance to ensure optimal performance.
- Reconfigure GCCS to regain processing capabilities for non-routine equipment malfunctions.
- Assist users in determining the cause of failures.
- Maintain licenses on the system as required.
- Manage mail and printer setups.

This new position closely matches the WWMCCS position of the informal system administrator at a WWMCCS site. However, managing a UNIX-based client/server system and network is much more complex and time consuming. It requires special skills, knowledge, and training. One of the key initial responsibilities of GSAs is implementing and advising on policies, CONOPs, and SOPs for GCCS administration. GCCS policies and technical SOPs are required because of the unique state of GCCS implementation. GSAs must be actively involved in these policy and procedural preparation activities involving system administration at their sites.

6.2.4 GCCS Database Administrator (GDBA). The GDBA is responsible for the day-to-day operations of the databases at the GCCS site, including the database server (SUN SPARCserver 1000 or 2000) running the Oracle RDBMS, or the EM application using the Sybase RDBMS, or the AMHS server application using the Verity Topic RDBMS. If the site has none of these databases, the position may be vacant. The *GCCS System Administration Manual* covers Sybase administration (Section 11), Executive Manager Operations (Section 22), AMHS Administration (Section 19), and Oracle RDBMS Overview (Appendix A), which includes GCCS database information. This position most closely matches the responsibilities of the WWMCCS TDBM and the WWMCCS site database personnel (site TDBM). The database support may extend to a number of different applications and databases. Some of the duties of the GDBA are:

- Coordinate incremental/partial back-ups of the databases with the GSC and the GMC-Pentagon.
- Generate periodic summaries of database performance and utilization.
- Coordinate and maintain database modifications.
- Monitor all database applications for proper performance.
- Manage disk/tape storage.

6.2.5 GCCS Site Designated Approving Authority (DAA). The site DAA is responsible for local policies and guidance to ensure the integrity and security of the GCCS operations. The DAA is responsible for accrediting GCCS at the site. These duties are similar to those of the site DAA who supported

WWMCCS.

6.2.6 Site GCCS Security Officer (SGSO). The SGSO is responsible for ensuring the integrity and security of the local GCCS system and network. This position was previously known as the WASSO. The SGSO is responsible for providing security information to the GCCS Site DAA. The SGSO's duties are defined in CJCSI 6731.01 and include establishing and maintaining user accounts and passwords. Version 2.1 documents useful to the SGSO include:

- *GCCS Policy*, dated December 1994.
- *GCCS Automated Information System (AIS) Security Plan*, dated 15 June 1995. (LL-500-67-04)
- *GCCS System Security Implementation Instructions for Site Security Administrators*, dated 12 May 1995. (LL-500-43-04)
- *JDISS Security Concept of Operations*, 15 February 1995. (LL-210-08-02)
- *JMCIS 2.1 Security Manager's Guide*, dated 15 July 1994. (LL-211-11-01)

6.2.7 GCCS Technical Support Point of Contact (GSSP). The technical support position supports the GSA in maintaining the GCCS applications, providing local user support, and troubleshooting site problems. Multiple persons may fill this site position as it requires various areas of expertise dealing with the COE, software principles, etc. The following tasks are typical:

- Assists in determining the cause of failures.
- Prepares training material and train site personnel.
- Maintains system and application configuration parameters.
- Maintains GCCS applications.

6.2.8 User Permissions. GCCS users have a responsibility to ensure they meet the requirements necessary to obtain access to the GCCS assets needed to perform their mission. The site GSA and security personnel administer the systems for account codes and user IDs, STU-II controls, etc. However, users must understand the requirements before a crisis situation in which they may unexpectedly need to use an unfamiliar site asset or use a back-up site asset. Besides the security requirements, the GCCS client/server environment also requires user permissions be in place to allow use of the various components of GCCS. Figure 6-7 addresses the problem and presents a case to demonstrate which permissions, profiles, etc. are required for the case concerned. It is intended to highlight the general requirement to ensure all steps have been taken to access the GCCS. All situations cannot be covered. Rather, GCCS users should address questions to their site GSA, GNA and GSSP, and security personnel.

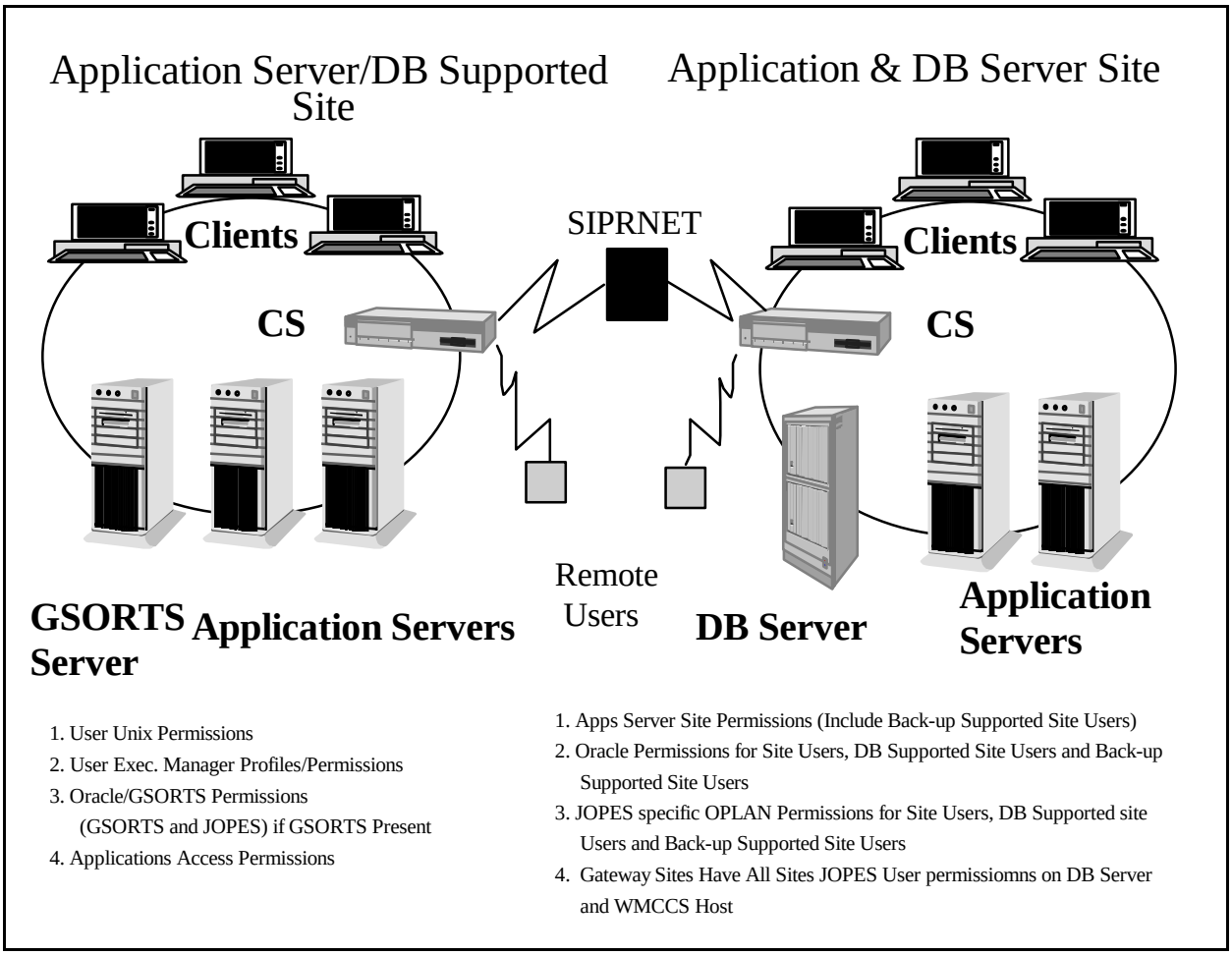

Figure 6-7. Required GCCS Permissions

6.3 Crisis Response

There were five WIN Modes of Operation in the WWMCCS environment. A minimize procedure was also applied to the DSNET2, which was dedicated to supporting WWMCCS. This is no longer true in the GCCS environment since GCCS users only comprise 15 percent of the SIPRNET subscribers. This section discusses the use of GCCS during periods of increasing Operations Tempo i.e., the transition to go-to-war GCCS. Subjects include: how transition is announced, how priorities are established and maintained, and how site responsibilities are determined. Communications aspects are also discussed.

GCCS also uses a priority mode concept but it is limited to the GCCS sites and does not include communications. GCCS operations are in two categories, Routine Mode and Priority Mode. Routine Mode covers day-to-day operations while Priority Mode covers five levels of exercise or crises situations. The five levels within the Priority Mode are defined in Table 6-2.

Table 6-2. Priority Levels within the GCCS Priority Mode

Priority Level	Condition	Command Authority
1	Worldwide Crisis	As Directed by the Director, J-3, the Joint Staff
2	Regional or Local Crisis	As Announced by the GMC-Pentagon upon Recommendation of the Regional CINC in Coordination with the Director, J-3, the Joint Staff
3	JCS Exercise	As Directed by the Director, J-3, the Joint Staff
4	Command Exercise	As Announced by the GMC-Pentagon upon Recommendation of the CINC in Coordination with the Data Information Coordination Officer (DICO) [9]
5	Command Special Operation	As Directed by the CINC with notification to the GMC Director

During Priority Mode, all GCCS site operations are under control of the J3 DICO. The J3 DICO can determine or limit the types of applications executed at GCCS sites, the priority of site repairs, manning requirements, and other actions critical to operations of GCCS. Only those authorities designated in the Table have authority to declare a Priority Mode. When a Priority Mode is declared, the J3 DICO will inform and assume command of all concerned sites.

Priority Mode declaration will usually be via an AUTODIN message and will identify the sites concerned, since not all GCCS sites may be involved. The message may also go directly to the concerned GCCS sites via e-mail over the SIPRNET and via the GCCS Management Center Conference (GMCCON) NewsGroup Teleconference. During Priority Mode, sites are required to comply with GMC-directed instructions for site restoration and trouble shooting actions within 15 minutes. If conditions preclude compliance within the 15-minute period, the local GCCS Site Coordinator must request resolution from the DICO.

As mentioned above, GCCS has no special priority over other subscribers to the SIPRNET. However, during Priority Modes levels 1 and 2, the GCCS Director has direct command authority over the DII/DISN GCC. The SIPRNET will normally be operated at no more than 60 percent of overall available bandwidth on the WAN structure, providing a 40 percent capacity to meet crises surge requirements. However, GCCS users should remember that the largest trunk capacity on the majority of SIPRNET trunks is 512 kbps. Although it is "wideband" compared to some low-speed subscriber circuits operating at 2.4 kbps, the 512 kbps is not wideband in today's communication environment. Users should remember that most GCCS applications require a minimum bandwidth of 32 kbps to operate properly. GCCS users should recognize that although operations on the local GCCS FDDI LAN are high-speed, external communications in time of crises will require bandwidth conservation for maximum efficiency, and GCCS operations over the SIPRNET may be restricted by the GCCS Director for that reason. This may particularly affect those sites involved in the crises since they are limited by the number of site gateways (Premise Router, serial port on the Communication

[9] The DICO is designated by the Director for Operations (J3), the Joint Staff and provides operational direction and guidance to GCCS. This position also exists in the WWMCCS environment.

Server, etc.) that can provide access to the SIPRNET.

6.4 Performance Adjustments

GCCS performance is monitored and controlled at several levels and GCCS users should be sensitive to changes in performance. Overall system performance will be monitored by the GMC-Pentagon. The GMC-Pentagon will gather statistics on the entire GCCS, including utilization rates between the GCCS premise router and the SIPRNET WAN, data and application server failure rates, and AMHS availability data. The GMC-Pentagon will use automated data gathering devices and software to gather performance data for each GCCS site as well as data reported separately by the GSC. The GMC will direct overall changes at the GCCS system/network level to make needed performance adjustments. The GMC-Pentagon will provide daily, weekly, and monthly reports to the GCCS DIR and monthly to GCCS sites. Historical files will be maintained for analysis purposes. The GCCS Engineering office develops performance criteria and determines thresholds for measurement purposes.

Local GCCS site performance is monitored by the GSA and the GDBA. The GSA will monitor total system performance. The GDBA will monitor database applications for poor performance and will generate periodic summaries of database performance and utilization. GCCS site-controllable performance adjustments are in the domain of these individuals. Procedures for adjusting performance are contained in system documents such as the *GCCS System Administration Manual* and commercial manuals such as the Oracle manuals.

GCCS users should be aware of and report any degradation in system performance. Some user actions can affect performance. The GSA may notice changes in performance and may direct users to adjust their usage to correct performance problems. A user might create an ill-formed, inefficient query or generate an intensive or long-running transaction. The GSA might request the user perform an activity during a less busy time period.

6.5 Obtaining Help

The primary sources of technical help are identified in Sections 4.4.1.1, 6.1.5.3, 6.1.5.4, 6.1.5.5, 7.0, and Appendix A. In addition, many of the applications contain help information accessible through the various menus. The GMC-JOPES personnel can provide assistance regarding JOPES applications. Local site GSA and GDBA can help with applications problems in a similar role performed by the WWMCCS site TDBM and FDBM.